REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks.

Claims 1-40 are pending in the application, with claims 1, 18, and 31 being independent. Claims 31 and 38 have been amended. No new matter has been added.

§ 103 REJECTIONS

Reeds in view of Greene

Claims 1-10, 13-25, 28-37 and 40 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 5,724,427 (Reeds) in view of U.S. Patent No. 6,646,639 (Greene). Applicant respectfully traverses the rejection.

Independent claim 1, as presented recites,

> A method comprising:
> sequentially storing a plurality of results provided by a stream cipher output rule in a first, second, and third storage units;
> providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third storage units that are at least a threshold value apart; and
> upon reaching the threshold value of the output rule results, serially rotating contents of the first, second, and third storage units.

Reeds is directed to a particular method and apparatus for encrypting text using an autokeyed rotational state vector (Reeds, Abstract), and was cited for its alleged teaching of "sequentially storing a plurality of results provided by a stream cipher" (Office Action, page 2). The plain text to be encrypted in Reeds is "stored as a block in a buffer" and then "each byte of plain text in the buffer [is] encrypted to yield a byte of cipher text."

(Reeds, Abstract and Fig. 4.) "RAM 735 advantageously is used to store information which is updated or which is dynamic, such as the rotational state vector, the key and the buffer containing text for encryption or decryption." (Reeds, Column 10, lines 4-7.) While Reeds appears to buffer the text to be processed, Reeds makes no mention of storing the processed results.

As described above, Reeds discloses storing input to a stream cipher, but fails to disclose or suggest "sequentially storing a plurality of results provided ***by*** a stream cipher output rule," (emphasis added) as presently recited in claim 1. Additionally, Reeds fails to disclose or suggest "a first, second, and third storage units" as also presently recited in claim 1.

Reeds was also cited for its alleged teaching of "a pairing function, the pairing function pairing individual values from the first and third storage units." (Office Action, page 2.) Reeds discusses using a pairing function of letters via its rotational state vector as described below:

> In Fig. 3 encryption processor 320 encrypts a byte of text in b to generate a byte of cipher text in c using input from translation table 330 and from rotational state vector 310. In encrypting a stream of plain text, values of elements in rotational state vector are then changed as a function of one or more of: the plain text byte or the cipher text byte.
>
> (Reeds, Column 7, lines 20-31.)

However, Reeds fails to teach or suggest "storing a plurality of results provided ***by*** a stream cipher output rule" (emphasis added) and then "providing a plurality of results from a pairing function" as presently recited in claim 1. Indeed, as described above, Reeds makes no mention of even storing the output, which would be necessary to perform the operation disclosed in this application, let alone manipulating it.

Additionally, while the rotational state vector in Reeds may be changed as a function of the input or output text, Reeds does not appear to disclose taking the resulting output text and introducing an additional function introduced to reduce the correlation between outputs. Thus, Reeds fails to suggest or disclose "the pairing function pairing individual values from the first and third storage units that are at least a threshold value apart" or once that pairing has been accomplished "serially rotating contents of the first, second, and third storage units," both as presently recited in claim 1.

Greene is directed to a method for improved occlusion culling in graphics systems (Greene, Title) and was cited for its alleged teaching of a "using the threshold value to determine whether to perform an arithmetic operation" (Office Action, page 3). However, Greene fails to remedy the deficiencies in Reeds noted above with respect to claim 1. For example, Greene fails to disclose or suggest "sequentially storing a plurality of results provided by a stream cipher output rule," as presently recited in claim 1.

Thus, Reeds and Greene, whether taken alone or in combination (assuming for the sake of argument that they can be combined), fail to disclose or suggest the features of claim 1. Accordingly, as discussed during the interview, independent claim 1 is allowable.

Dependent claims 2-10, and 13-17 depend from independent claim 1 and are allowable by virtue of this dependency, as well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

For example, **dependent claim 2** recites "wherein a short-term correlation between the individual values from the first and third storage units are limited." The Office asserts on page 3, that this feature is taught by Greene. However, the cited portion of Greene merely discloses "the order of boxes on the lists is the order in which their visibility was established, which is often correlated with occlusion order...." (Greene, Column 41, lines 60-61.) As discussed above with respect to claim 1, Greene does not disclose or suggest "sequentially storing a plurality of results provided by a stream cipher output rule," let alone "wherein a short-term correlation between the individual values from the first and third storage units are limited," as presently recited in dependent claim 2. Accordingly, claim 2 is allowable for at least this additional reason.

For example, **dependent claim 3** recites "wherein a length of each of the first, second, and third storage units equals the threshold value." The Office asserts on page 3, that this feature is taught by Greene. However, the cited portion of Greene merely discloses "if the maximum "z advance" is less than some specified positive threshold value, call it zdelta..." (Greene, Column 24, lines 57-58.) As discussed above with respect to claim 1, Greene does not disclose or suggest "sequentially storing a plurality of results provided by a stream cipher output rule," let alone "wherein a length of each of the first, second, and third storage units equals the threshold value," as presently recited in dependent claim 3. Accordingly, claim 3 is allowable for at least this additional reason.

For example, **dependent claim 4** recites "wherein the first, second, and third storage units are implemented in a single memory device." The Office asserts on page 4, that this feature is taught by Reeds and Greene. As discussed above with respect to claim

1, Reeds fails to disclose or suggest "a first, second, and third storage units," as presented in claim 1. No specific citation was made to Greene, however Greene does not disclose or suggest "sequentially storing a plurality of results provided by a stream cipher output rule," let alone "wherein the first, second, and third storage units are implemented in a single memory device," as presently recited in dependent claim 4. Accordingly, claim 4 is allowable for at least this additional reason.

For example, **dependent claim 5** recites "wherein the serial rotation is performed by shifting the first, second, and third storage units in a same direction." The Office asserts on page 4, that shifting is taught by Reeds. As discussed above with respect to claim 1, Reeds fails to disclose or suggest "a first, second, and third storage units," as presented in claim 1. Given Reeds' lack of storage units, Reeds could not teach shifting them. The Office asserts on page 4, that this feature is taught by Greene as well. However, the cited portion of Greene merely discloses "transforming a linear equation from the coordinate frame of one tile to the coordinate frame of a "child" tile involves translation and scaling computations, where scaling is performed by shifting." (Greene, Column 27, lines 10-18.) However, Greene does not disclose or suggest "sequentially storing a plurality of results provided by a stream cipher output rule," let alone "wherein the serial rotation is performed by shifting the first, second, and third storage units in a same direction," as presently recited in dependent claim 5. Accordingly, claim 5 is allowable for at least this additional reason.

For example, **dependent claim 9** recites "wherein the first and third storage units are initialized with random values." The Office asserts on page 4, that this feature is taught by Reeds. Reeds discloses "initializing the rotational state vector as a function of

a key." (Reeds, Column 5, lines 58-59.) However, Reeds fails to disclose "wherein the first and third storage units are initialized with random values," as presently recited in dependent claim 9. Accordingly, claim 9 is allowable for at least this additional reason.

Independent claim 18 was also rejected under § 103(a), and as presented recites,

> A system comprising:
> a processor;
> a system memory coupled to the processor;
> sequentially storing a plurality of results provided by a stream cipher output rule in a first, second, and third portion of the system memory;
> providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third portions of the system memory that are at least a threshold value apart; and
> upon reaching the threshold value of the output rule results, serially rotating contents of the first, second, and third portions of the system memory.

Reeds is directed to a particular method and apparatus for encrypting text using an autokeyed rotational state vector. (Reeds, Abstract.) Similar to claim 1 above, Reeds was cited for its alleged teaching of "sequentially storing a plurality of results provided by a stream cipher" (Office Action, page 2). The plain text to be encrypted in Reeds is "stored as a block in a buffer" and then "each byte of plain text in the buffer [is] encrypted to yield a byte of cipher text." (Reeds, Abstract and Fig. 4.) "RAM 735 advantageously is used to store information which is updated or which is dynamic, such as the rotational state vector, the key and the buffer containing text for encryption or decryption." (Reeds, Column 10, lines 4-7.) While Reeds appears to buffer the text to be processed, Reeds makes no mention of storing the processed results.

As described above, Reeds discloses storing input to a stream cipher, but fails to disclose or suggest "sequentially storing a plurality of results provided ***by*** a stream cipher output rule," (emphasis added) as presently recited in claim 18. Additionally, Reeds fails to disclose or suggest "a first, second, and third portion of the system memory" as also presently recited in claim 18.

Reeds was also cited for its alleged teaching of "a pairing function, the pairing function pairing individual values from the first and third storage units." (Office Action, page 2.) Reeds discuses using a pairing function of letters via its rotational state vector as described below:

> In Fig. 3 encryption processor 320 encrypts a byte of text in b to generate a byte of cipher text in c using input from translation table 330 and from rotational state vector 310. In encrypting a stream of plain text, values of elements in rotational state vector are then changed as a function of one or more of: the plain text byte or the cipher text byte.
>
> (Reeds, Column 7, lines 20-31.)

However, Reeds fails to teach or suggest "sequentially storing a plurality of results provided ***by*** a stream cipher output rule" (emphasis added) and then "providing a plurality of results from a pairing function" as presently recited in claim 18. Indeed, as described above, Reeds makes no mention of even storing output, which would be necessary to perform the operation disclosed in this application, let alone manipulating it.

Additionally, while the rotational state vector in Reeds may be changed as a function of the input or output text, Reeds does not appear to disclose taking the resulting output text and introducing an additional function introduced to reduce the correlation between outputs. Thus, Reeds fails to suggest or disclose "the pairing function pairing individual values from the first and third portions of the system memory that are at least a

threshold value apart" or once that pairing has been accomplished "upon reaching the threshold value of the output rule results, serially rotating contents of the first, second, and third portions of the system memory," both as presently recited in claim 18.

Greene is directed to a method for improved occlusion culling in graphics systems (Greene, Title) and was cited for its alleged teaching of a "using the threshold value to determine whether to perform an arithmetic operation" (Office Action, page 3). However, Greene fails to remedy the deficiencies in Reeds noted above with respect to claim 18. For example, Greene fails to disclose or suggest "sequentially storing a plurality of results provided by a stream cipher output rule in a first, second, and third portion of the system memory," as presently recited in claim 18.

Thus, Reeds and Greene, whether taken alone or in combination (assuming for the sake of argument that they can be combined), fail to disclose or suggest the features of claim 18. Accordingly, independent claim 18 is allowable.

Dependent claims 19-25, and 28-30 depend from independent claim 18 and are allowable by virtue of this dependency, the similar arguments as to those made above, as well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

Independent claim 31 was also rejected under § 103(a). Applicant respectfully traverses the rejection. Nevertheless, without conceding the propriety of the rejection and in the interest of expediting allowance of the application, claim 31 has been amended and is believed to be allowable. Claim 31 as currently amended recites,

One or more computer-readable media having instructions stored thereon that, when executed, direct a machine to perform acts comprising:

strengthening an existing stream cipher's output by sequentially storing a plurality of results provided by the stream cipher in a first, second, and third storage units;

providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third storage units that are at least a threshold value apart;

upon reaching the threshold value of the existing stream cipher output, serially rotating contents of the first, second, and third storage units, thereby strengthening the cipher stream; and

outputting the now strengthened stream cipher.

For reasons similar to those given above in claims 1 and 18, Reeds to disclose or suggest "strengthening an existing stream cipher's output by sequentially storing a plurality of results provided by the stream cipher in a first, second, and third storage units," as presently recited in independent claim 31.

Similar to claims 1 and 18, Greene fails to remedy the deficiencies in Reeds noted above with respect to claim 31. For example, Greene fails to disclose or suggest "strengthening an existing stream cipher's output by sequentially storing a plurality of results provided by the stream cipher in a first, second, and third storage units," as presently recited in claim 31.

Thus, Reeds and Greene, whether taken alone or in combination (assuming for the sake of argument that they can be combined), fail to disclose or suggest the features of claim 31. Accordingly, independent claim 31 is allowable.

Dependent claims 32-37, and 40 depend from independent claim 31 and are allowable by virtue of this dependency, the similar arguments as to those made above, as

well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

Reeds in view of Greene and further in view of Petersen

Claims 11-12, 26-27, 38-39 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 5,724,427 (Reeds) in view of U.S. Patent No. 6,646,639 (Greene) and further in view of U.S. Patent No. 7,170,997 (Petersen). Applicant respectfully traverses the rejection.

Dependent claims 11 and 12 depend from independent claim 1 and include all the features of that claim. Peterson discloses a method of generating pseudo-random numbers (Peterson, Title), and was cited for its alleged teaching of a random walk (Office Action, page 5). However, Peterson fails to remedy the deficiencies in Reeds and Greene as noted above with respect to claim 1. For example, Peterson fails to disclose or suggest "sequentially storing a plurality of results provided by a stream cipher output rule in a first, second, and third storage units" or "providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third storage units that are at least a threshold value apart; and upon reaching the threshold value of the output rule results, serially rotating contents of the first, second, and third storage units" as presently recited in claim 1. Therefore, claims 11 and 12 are allowable by virtue of their dependence from independent claim 1, as well as for the additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

Dependent claims 26 and 27 depend from independent claim 18 and include all the features of that claim. Peterson discloses a method of generating pseudo-random numbers (Peterson, Title), and was cited for its alleged teaching of a random walk (Office Action, page 5). However, Peterson fails to remedy the deficiencies in Reeds and Greene as noted above with respect to claim 18. For example, Peterson fails to disclose or suggest "sequentially storing a plurality of results provided by a stream cipher output rule in a first, second, and third portion of the system memory" or "providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third portions of the system memory that are at least a threshold value apart; and upon reaching the threshold value of the output rule results, serially rotating contents of the first, second, and third portions of the system memory," as presently recited in claim 18. Therefore, claims 26 and 27 are allowable by virtue of their dependence from independent claim 18, as well as for the additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

Dependent claims 38 and 39 depend from independent claim 31 and include all the features of that claim. Nevertheless, without conceding the propriety of the rejection, and in the interest of expediting allowance of the application, claims 31 and 38 have been amended and are believed to be allowable.

Peterson discloses a method of generating pseudo-random numbers (Peterson, Title) and was cited for its alleged teaching of using random walks (Office Action, page 5). However, Peterson fails to remedy the deficiencies in Reeds and Greene as noted above with respect to claim 31. For example, Peterson fails to disclose or suggest

"strengthening an existing stream cipher's output by sequentially storing a plurality of results provided by the stream cipher in a first, second, and third storage units" or "providing a plurality of results from a pairing function, the pairing function pairing individual values from the first and third storage units that are at least a threshold value apart; and upon reaching the threshold value of the output rule results, serially rotating contents of the first, second, and third storage units," as presently recited in claim 31. Therefore, claims 38 and 39 are allowable by virtue of their dependence from independent claim 31, as well as for the additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

CONCLUSION

For at least the foregoing reasons, claims 1-40 are in condition for allowance. Applicant respectfully requests reconsideration and withdrawal of the rejections and an early notice of allowance.

If any issue remains unresolved that would prevent allowance of this case, **Applicant requests that the Examiner contact the undersigned agent to resolve the issue**.

Respectfully submitted,

Date: 1/7/08

By:
Dominic S. Lindauer
Reg. No. 61,417